AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means ❒ Original ❒ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Information associated with YouTube channel UC62TCz6JDjwzqnY6Jq18EKg and email accounts clustergeek64@gmail.com and hounddowg1@gmail.com (the "accounts"), as well as all Google, LLC accounts linked to these accounts by cookie values, creation IP addresses, recovery email, SMS recovery, device, telephone numbers, and other similar identifiers, that is stored at premises owned, maintained, controlled, or operated by Google, LLC more fully described in attachment A	)	Case No.23-948M(NJ)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____
(identify the person or describe the property to be searched and give its location):

see Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

see Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 7/21/2023 *(not to exceed 14 days)*

❒ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Nancy Joseph .
(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____ .

Date and time issued: 7/7/2023 @ 4:04 p.m.

Nancy Joseph
Judge's signature

City and state: Milwaukee, WI

U.S. Magistrate Nancy Joseph
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with YouTube channel UC62TCz6JDjwzqnY6Jq18EKg and email accounts clustergeek64@gmail.com and hounddowg1@gmail.com (the "accounts"), as well as all Google, LLC accounts linked to these accounts by cookie values, creation IP addresses, recovery email, SMS recovery, device, telephone numbers, and other similar identifiers, that is stored at premises owned, maintained, controlled, or operated by Google, LLC, a company headquartered at 1600 Amphitheater Parkway, Mountain View, CA 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google LLC (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to requests made under 18 U.S.C. § 2703(f) on or about July 22, 2022, and June 23, 2023, the Provider is required to disclose to the government the following information from August 1, 2019, to the present for each account or identifier listed in Attachment A:

Google Account

- **SUBSCRIBER AND ACCESS RECORDS:** All business records and subscriber information, in any form kept, pertaining to the account, including: full name; physical address; telephone numbers, including SMS recovery and alternate sign-in numbers; alternative and recovery email addresses, including those provided during registration; usernames, screennames and other identifiers; account status; account creation date; account registration IP address; length of service; records of session times and durations, including log-in IP addresses; methods of connecting; log files; subscriber change history; means and source of payment (including any credit or bank account number); and detailed billing records;
- **DEVICES:** All device information associated with the accounts, including but not limited to, manufacture names, model numbers, serial number, media access control (MAC) addresses, international mobile equipment identifier (IMEI) numbers, FCC ID numbers, Android IDs, and telephone numbers;
- **SERVICES:** The types of services utilized, including connected applications and sites, and any dates associated with the commencement or termination of that use;
- **FORWARDING OR FETCHING ACCOUNTS:** All forwarding or fetching accounts relating to the accounts;

- **BROWSING, SEARCH, and APPLICATION USE HISTORY:** All Internet search, browsing history, and application usage history, such as Web & App Activity**,** including: search terms; browsing history, including application usage; bookmarks; passwords; autofill information; alerts, subscriptions, and other automated searches, including associated notifications and creation dates; all text typed into the Google Chrome address bar or Google search bar, including URLs and IP addresses; all URLs or IP addresses clicked on; user settings; and all associated logs and change history;

- **LOCATION HISTORY:** All records indicating the location at which the account was active, such as Location History and Web & App Activity, including: GPS data; cell site/cell tower information; IP addresses; information associated with each location record, including the source of the data, date and time, latitude and longitude, estimated accuracy, device and platform, and inferences drawn from sensor data (such as whether a user was at rest, walking, biking, or in a car); and associated logs and user settings, including Timeline access logs and change history;

Gmail

- **GMAIL:** The contents of all emails associated with the account, including, but not limited to: stored or preserved copies of emails sent to and from the account, draft emails, and deleted emails; attachments; the source and destination addresses associated with each email; the date and time at which each email was sent; the size and length of each email; and true and accurate header information including the actual IP addresses of the sender and recipients of the emails;

- **CONTACTS:** Any records pertaining to the user's contacts, including: address books; contact lists, including autocomplete suggestions; social network links; groups, including Google Groups to which the user belongs or communicates with; user settings; and all associated logs and change history;

- **CALENDAR:** Any records pertaining to the user's calendar, including: Google Calendar entries; Google Tasks; reminders; appointments; invites; and goals; the sender and recipients of any event invitation, reminder, appointment, or task; user settings; and all associated logs and change history;

- **WEB-BASED CHATS:** The contents of all chats associated with the account, including Google Hangouts, Meet, and Chat, in any format (text, audio, or video) including, but not limited to: stored, deleted, and draft chat communications, including attachments and links; the source and destination addresses associated with each communication, including IP addresses; the size and length of each communication; user settings; and all associated logs, including access logs and change history;

Google Drive

- The contents of all records associated with the account in Google Drive (including Docs, Sheets, Forms, and Slides) and Google Keep, including: files, folders, media, notes, lists, applications, and other data uploaded, created, stored, or shared with the account including drafts and deleted records; third-party application data and backups; SMS data

and device backups; the creation and change history of each record; accounts with access to or which previously accessed each record; any location, device, other Google service (such as Google Classroom or Google Group), or third-party application associated with each record; and all associated logs, including access logs and IP addresses, of each record;

Google Photos

- The contents of all media associated with the account in Google Photos or Picasa, including: photos, GIFs, videos, animations, collages, icons, or other data uploaded, created, stored, or shared with the account, including drafts and deleted records; third-party data; the creation and change history of each record; accounts with access to or which previously accessed each record; any location, device, or third-party application data associated with each record; and all associated logs, including access logs and IP addresses, of each record;

Google Maps and Trips

- All maps data associated with the account, including Google Maps and Google Trips, including: all saved, starred, and privately labeled locations; search history; routes begun; routes completed; mode of transit used for directions; information associated with locations and other data associated with My Maps and Location Sharing; accounts and identifiers receiving or sending Location Sharing information to the account; changes and edits to public places; and all associated logs, including IP addresses, location data, and timestamps, and change history;

Google Play Store

- All activity relating to Google Play, including: downloaded, installed, purchased, used, and deleted applications, movies, music, television shows, books, magazines, games, and other files; details of the associated device and Android ID for each application, medium, or file; payment transactions; user settings; and all associated logs, including IP addresses, location data, timestamps, and change history;

Messaging Services

- **MOBILE MESSAGING:** The contents of all messages associated with the account, including Google Duo, Android Messages, and Google Allo, in any format (e.g. SMS, MMS, or RCS) including, but not limited to: stored, deleted, and draft messages, including attachments and links; the source and destination addresses associated with each communication, including IP addresses and telephone numbers; the size and length of each communication; associated telephone numbers, including SMS recovery numbers; usernames and other identifiers; user settings; and all associated logs and change history;

YouTube

- **YOUTUBE CONTENTS:** The contents of all media associated with the account on YouTube, whether active, deleted, or in draft, including: copies of videos and other

media only if uploaded to, saved to, shared by or shared with the account; edits, comments, likes, chats, and other interactions, including associated URLs; search history; channels; subscriptions; subscribers, friends, and other contacts; playlists; connected applications; associated URLs for each record; creation and change history; privacy settings for each record; and all associated logs, including IP addresses, locations, timestamps, and device identifiers;

- **YOUTUBE WATCH HISTORY:** A record of the account's watch history, including: accessed URLs and their associated duration, privacy settings, upload timestamps, tags, IP addresses, change history, location information, and uploading account or identifier; the logs for each access by the account, including IP address, location, timestamp, and device identifier; and change history;

- **YOUTUBE SUBSCRIBER RECORDS:** All business and subscriber records associated with the account on YouTube, including birthday; name; username and other identifiers; linked accounts; alternate or recovery emails; telephone numbers, including SMS recovery numbers; physical addresses; account status; account creation date; account registration IP address; length of service; means and source of payment (including any credit or bank account number); associated devices; associated Android IDs; and associated logs and change history;

AdSense and AdWords

- **ADWORDS/GOOGLE ADS:** All records for advertising transactions by the account relating to Google Ads, AdWords, and DoubleClick for Advertisers, including: bid, location of advertisement (including URL), permitted advertisements, blocked advertisements, design and customization settings, and engagement records; payment transactions; user settings; and all associated logs, including IP addresses, location data, timestamps, and change history;

- **ADVERTISING SUBSCRIBER RECORDS:** All business and subscriber records associated with the account on AdSense, Google Ads, Adwords, and DoubleClick by Google, including: name; user name; physical address; alternate or recovery emails; telephone numbers, including SMS recovery numbers; linked accounts; account status; account creation date; account registration IP address; length of service; associated devices; associated AndroidIDs; means and source of payment (including any credit or bank account number); and all associated logs and change history;

Connected Applications and Accounts

- **LINKED NON-GOOGLE ACCOUNTS:** All records relating to connected applications and websites not controlled by Google, including: applications and websites connected to the account at any time; associated account identifiers; privacy settings and account access permissions; and all associated logs, including access logs using Google credentials, timestamps, IP addresses, and change history;

The Provider is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and/or instrumentalities of violations of 18 U.S.C. § 842(p) (teaching or demonstrating the making or use of weapons of mass destruction) involving James Morgan (aka Karactus Blome) and occurring after August 1, 2019, including, for each account or identifier listed on Attachment A, information referring or relating to the following matters:

(a) Records of communications related to public and private comments posted to YouTube channel UC62TCz6JDjwzqnY6Jq18EKg including official copies of all videos posted and deleted;

(b) The identity of the person(s) who created or used the accounts, including records that help reveal the whereabouts of such person(s);

(c) Evidence indicating how and when the accounts were accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the account owner;

(d) Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information); and

(e) Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information associated with YouTube channel UC62TCz6JDjwzqnY6Jq18EKg and email accounts clustergeek64@gmail.com and hounddowg1@gmail.com (the "accounts"), as well as all Google, LLC accounts linked to these accounts by cookie values, creation IP addresses, recovery email, SMS recovery, device, telephone numbers, and other similar identifiers, that is stored at premises owned, maintained, controlled, or operated by Google, LLC more fully described in attachment A

Case No.23-948M(NJ)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

see Attachment A.

located in the _____ District of _____, there is now concealed *(identify the person or describe the property to be seized)*:

see Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 842(p)	teaching or demonstrating the making or use of weapons of mass destruction

The application is based on these facts:

see attached affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

JUSTIN MOSIMAN Digitally signed by JUSTIN MOSIMAN Date: 2023.07.05 17:01:16 -05'00'

Applicant's signature

FBI SA Justin Mosiman

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 7/7/2023

Judge's signature

City and state: Milwaukee, WI

U.S. Magistrate Judge Nancy Joseph

Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Justin Mosiman, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with accounts, YouTube channel UC62TCz6JDjwzqnY6Jq18EKg and email addresses clustergeek64@gmail.com and hounddowg1@gmail.com, that is stored at premises controlled by Google LLC ("Google"), 1600 Amphitheater Parkway, Mountain View, CA 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation and have been since May 2019. I have also been a Special Agent Bomb Technician since February 2021. I am currently assigned to the Joint Terrorism Task Force in Milwaukee, where I investigate violations of federal law. I have investigated and assisted in the investigation of matters involving violations of federal law related to counterterrorism and domestic terrorism, including the service of search and arrest warrants. Prior to my employment with the FBI, I served in the U.S. Navy for six years as an Explosive Ordnance Disposal Technician and provided contract support as an Explosive Ordnance Disposal Subject Matter Expert to the Department of Defense and Department of Energy for twelve years collectively.

3. The facts in this affidavit are known to me through my personal knowledge, training, experience, and through information provided to me by other law enforcement officers in the course of

their official duties, whom I consider to be truthful and reliable.

4. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 842(p) (teaching or demonstrating the making or use of weapons of mass destruction) have been committed by James Morgan (formerly known as Karactus Blome).[1] There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is a district court of the United States that has jurisdiction over the offenses being investigated.

PROBABLE CAUSE

7. Blome lived with his mother and stepfather in Wheeling, Illinois, until August 2019, when he moved into his father's residence in Janesville, Wisconsin.

8. During an interview in September 2019, a family member provided information that Blome acted in a racist and prejudicial manner toward all people of color, creeds, and ethnicities that are not Blome's own. The family member also stated that Blome had an extreme disdain for law enforcement, all forms of government, and all perceived authority. Since childhood, Blome had

[1] In December 2022, Blome petitioned for and was granted an order in Walworth County, Wisconsin, to change his name to James Morgan. In this affidavit, he will be referred to as Blome or Morgan, depending on when conduct occurred.

difficulties with physical and verbal altercations due to extreme anger management issues. Later, in October 2019, the family member provided an additional general concern that Blome's anti-government behavior and rhetoric was accelerating after Blome moved to Janesville, Wisconsin, with his father.

9. An anonymous tip provided to the FBI in November 2019 by a Facebook friend of Blome claimed Blome posted a video on Facebook depicting how to produce an acid gun to shoot sulfuric acid and stated in the video "governments should be afraid of their people. So here's how you make a device that shoots sulfuric acid!"

10. Blome contacted the Wisconsin Department of Justice (Wisconsin DOJ) on November 5, 2019, after being notified by his father that the Wisconsin DOJ and the Janesville Police Department unsuccessfully attempted to contact Blome. During the interview, Blome admitted making several homemade weapons as means to protect himself before abruptly ending the phone call.

11. Open-source searches revealed social media accounts linked to James Morgan (aka Karactus Blome), including a YouTube channel UC62TCz6JDjwzqnY6Jq18EKg, Facebook accounts, and an Instagram account.

I. Choking Agent

12. Blome has posted on social media information about how to create, and has demonstrated the use of, a smoke powder or choking agent. On August 9, 2019, Blome posted a video on Facebook titled, "Blome Waffenkreationen – BWk," which translates from German as "Weapon Creations." In the video, Blome provided the ingredients to create sulfur dioxide/trioxide smoke powder and demonstrated the use of setting a chemical mixture aflame to create a smoke cloud. After stepping into the cloud to test the effects, he stated, "huge smoke cloud of a choking agent," and "looks

like I'm on the road to success then after all." Additionally, he provided clarifying instructions for the construction of the device.

13. On August 30, 2019, Blome published a YouTube video titled, "BWk- Sulfur X-Oxide Grenade Prototype Test." Blome demonstrated the use of the homemade chemical choking agent stating, "well that was a total success." At the end of the video, text states, "production to begin when I have funds."

14. On October 6, 2019, Blome posted to Facebook, "Everyone . . . I'm forming my own militia. We will be called . . . The New American Minutemen. We stand for freedom. Plain and Simple. We are decentralized. I created it, but it does not belong to me. . . . America has been losing their God given freedoms one by one. I intend to defend these. I am enraged. Our government taxes us endlessly, forces us to send our children to schools they control, control the press with their laws, and they've established over 700 imperialistic bases overseas and expect us to pay for them. . . . Seems like we need to dust off our guns and do this again, my fellow Americans. And if anything happens to me because I said this . . . well that should just prove our basic rights no longer exist. Who will answer this call to arms? Who's with me?"

15. On November 28, 2019, Blome posted on Facebook about an encounter he had with law enforcement regarding "weapons I invented." He stated, "I was a chemistry major in college . . . I know what I'm doing," "any gun I do ever have will be undocumented," and "Like I even really need a conventional weapon? I'm a weapon designer mf! I can likely invent something better anyway."

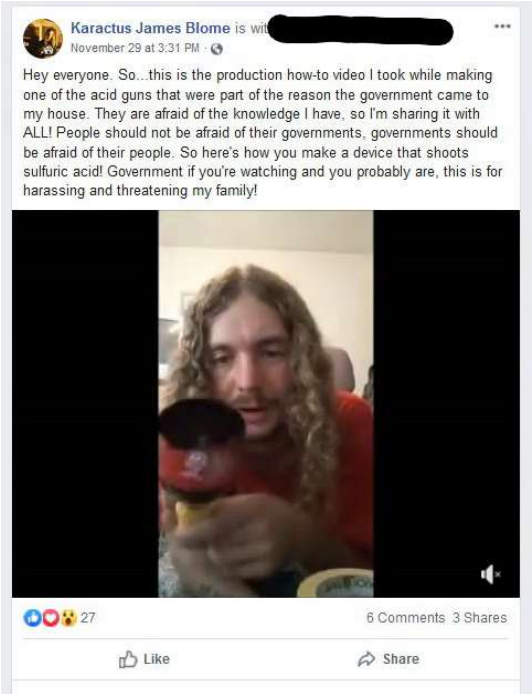
II. Acid Sprayer

16. Blome has also posted information about how to create, and demonstrated the use of, a device to spray sulfuric acid. Records provided from Duda Energy (www.dudadiesel.com) revealed that on July 15, 2019, Blome purchased two 950mL quantities of 98% concentration sulfuric acid.

17. On August 31, 2019, Blome posted a YouTube video titled, "BWk – XW-M2 Saurewerfer," (which translates from German as "Acid Thrower"). In the video, Blome showed multiple premade XW-M2 acid throwers and demonstrated how to use them to fire sulfuric acid. Later in the video he demonstrated how the sulfuric acid damages concrete and burns through clothing. The end of the video said, "Available for $10, acid not included. Sulfuric acid can be purchased at http://www.dudadiesel.com."

18. On November 29, 2019, Blome posted on Facebook a video about how to create and use a device to spray sulfuric acid. When posting the video, Blome stated, "this is the production how-to video I took while making one of the acid guns that were part of the reason the government came to my

house" and "People should not be afraid of their government, governments should be afraid of their people. So here's how you make a device that shoots sulfuric acid!"



19. On December 4, 2019, Blome posted a video on YouTube titled, "How to make a gun that shoots sulfuric acid." In the video Blome demonstrated how to create a device to spray sulfuric acid. He provided the name of "XWM2 Acid Thrower" or "Experimentalwaffe Modell Zwei Saurewerfer," which translates from German as "Experimental Weapon Model Two Acid Throwers." He stated the purpose is to shoot 98% pure sulfuric acid stating, "yeah, nasty stuff." He used black sealant and yellow tape to construct the device, stating that the color scheme was intentional like a bee or wasp to warn someone, "that I'm about to shoot something really nasty at you." He then demonstrated in the video how to fire the device and showed the damage the acid caused to concrete.

20. On January 12, 2023, the FBI Scientific Response and Analysis Unit provided an analysis of the acid thrower weapon. The report provided the chemical reactions depicted in the video are consistent with concentrated sulfuric acid. Additionally, the report provided that attacks involving acids are known to cause disfiguring skin injuries and blindness if splashed into the eyes.

III. Other Conduct

21. On January 19, 2020, Blome posted on Facebook, "I'm a loose cannon when I speak and I really don't have that much space between thought and action. Consequences often don't even register in my mind when I get heated, I just act."

22. In February and March 2020, Blome's Facebook friend (discussed above in paragraph 9) provided additional information to the FBI about Blome sending private Facebook messages stating he disliked the police and claiming he would be going after law enforcement and the government.

23. Purchase records provided by Classic Firearms of Indian Trail, North Carolina, revealed that on April 15, 2020, Blome purchased a Zastava Arms 7.62x39mm caliber AK-47 and had it shipped to CTR Firearms LLC in Janesville, Wisconsin.

24. The University of Wisconsin, Whitewater (UW-Whitewater) provided records showing that Blome has been enrolled since the fall of 2021 as an undergraduate in the College of Letters and Sciences. As of fall 2022, he had a 3.5 grade point average and was taking Chemistry II. In June 2022, Blome moved to an apartment in Whitewater, Wisconsin.

25. On May 18, 2022, Blome posted a video on Instagram under display name "karactusblome" with the location set as Janesville, Wisconsin, displaying multiple firearms and ammunition, including two bolt-action rifles, a semi-automatic rifle, a .44 caliber revolver, 7.5mm x 55mm ammunition, and multiple high-capacity drum ammunition magazines.

26. Purchase records provided from Atlantic Firearms in Bishop, Maryland, revealed that on June 10, 2022, Blome purchased a PTR-91 A3S .308 caliber rifle and had it shipped to CTR Firearms LLC in Janesville, Wisconsin.

27. On June 18, 2022, Blome posted on Instagram under display name "karactusblome" an image of himself holding a PTR-91 semi-automatic rifle. The caption of the image states, "My new

PTR 91. It's a high quality HK G3 battle rifle clone. Semi auto. Shoots .308 Winchester. Box mag holds 20 rounds, also accepts 50 and 100 round drums (which is my plan). Comes with that flash suppressor on the muzzle. Aperture rear sight, ring & post front sight. Bipod and optics are also planned."

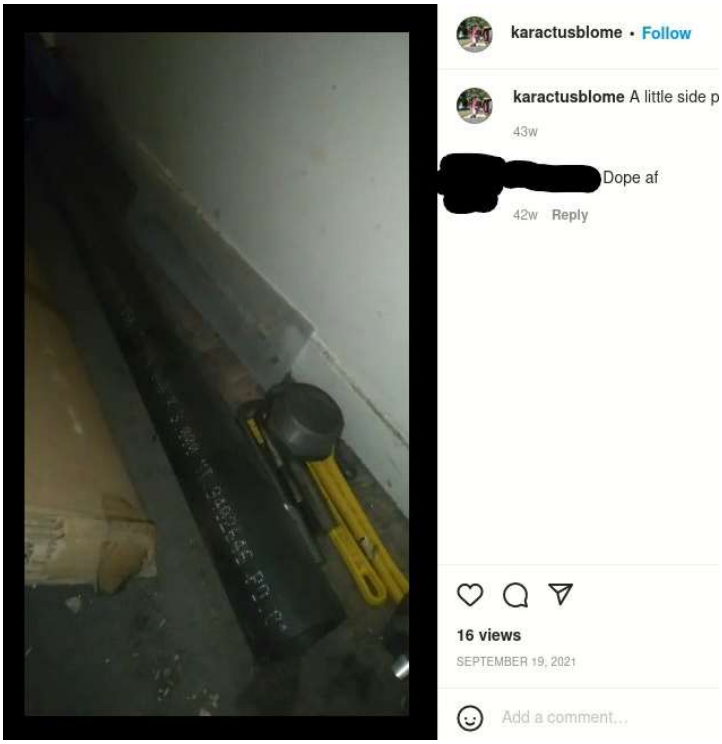
28. On June 29, 2022, Blome posted on Instagram under display name "karactusblome" an image of a PTR-91 .308 caliber semi-automatic rifle and two high-capacity drum magazines.

29. On July 1, 2022, Blome posted on Instagram under display name "karactusblome" a video displaying multiple firearms in his bedroom including a PTR 91 semi-automatic rifle with multiple drum magazines of ammunition, a .44 caliber revolver, and ammunition.

30. Financial records provided during the investigation revealed multiple firearms purchases by Blome from April 15, 2020, through June 10, 2022, totaling $2,813.32. Additionally, financial records revealed a total of $1,250 of expenditures from November 27, 2020, through July 2, 2022, at firearms and sporting goods stores for ammunition and firearms accessories.

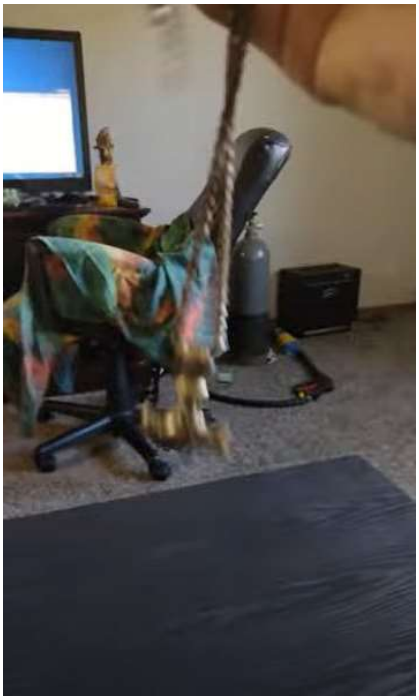
31. On October 6, 2022, Blome posted a video on YouTube titled, "Bean-Delete bison Chili." At 0:37 in the video, the book titled, "Anarchist Cookbook" is observed on the table. The Anarchist Cookbook contains various instructions on how to create and manufacture improvised weapons and explosives.

32. Blome has also revealed an intention to build and sell firearms, specifically a cannon-style weapon. On September 19, 2021, Blome posted on Instagram a video explaining his plan to build his own 7.62cm (3 inch) "cannon" using a large pipe, threaded breach plug, and ball projectiles. In the video, Blome stated, "I was planning to mass produce them" for about $1,000 to $1,500 each, making "artillery available to the common man" and "yes, I do intend to finish this project."



33. Blome has also revealed an intention to build a flamethrower. On May 12, 2022, Blome posted on YouTube a video titled, "Finishing up my Flamethrower." In the video he showed the components and design to create a gasoline flamethrower.

34. On August 26, 2022, Blome posted on YouTube a video titled, "My Daily Workout." At 5:10 in the video, the above flamethrower is in the background of what appears to be Blome's apartment in Whitewater, Wisconsin.



35. From November 2019 to December 2022, Morgan (formerly known as Blome) worked at Generac Power Systems in Whitewater, Wisconsin, on an assembly line as a painter and assembler for their commercial and residential backup power generator engines. In May 2023, a co-worker of Morgan at Generac stated that Morgan said he learned how to make bombs at school. Another co-worker voiced concern that Morgan would be "the first person to go postal" and often would stand away from the assembly line and talk to himself when not actively working on the assembly line. At other times, Blome would show up to work very angry and, in one instance, they recalled him slamming the engines against each other on the assembly line due to his anger.

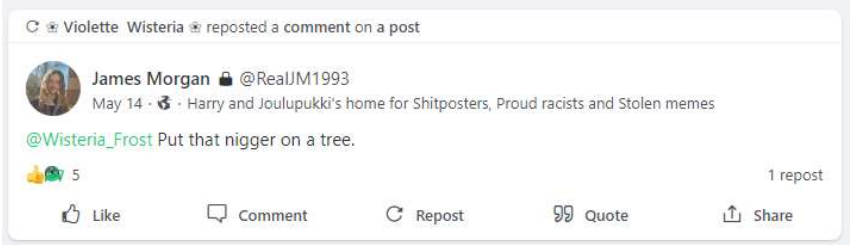
36. In May 2023, Morgan was interviewed by the FBI and Whitewater Police Department in relation to a reported missing person welfare check of an individual, C.L., that was requested by

Seabrook New Hampshire Police Department. During the interview, Morgan stated C.L. was his girlfriend and they met on the social media platform called Gab.

37. Records provided by Meta on August 8, 2022, revealed Facebook account 10001379619317 (username: krazy.karac, display name: Karactus James Blome) was closed on October 12, 2021. As of June 28, 2023, open-source searches revealed all other known Facebook and Instagram social networking accounts associated with Blome have been closed, including Facebook account 103661114323862 (username: Blome.Waffenkreationen) and Instagram account 41124491714 (Name: Karactus James Blome, vanity name: karactusblome). Facebook and Instagram are known to permanently and temporarily close accounts that violate their terms and conditions for speech. Due to Meta policies, extremists are known to stop using Meta platforms in order to use more derogatory speech. Additionally, due to Meta's terms and conditions, extremists are known to depart from using Meta platforms to prevent being reported to law enforcement or to delete evidence of crimes.

38. Records provided by Gab in June 2023 revealed James Morgan as the subscriber for username @RealJM1993 (display name James Morgan), which was created on January 21, 2021. Morgan stated in the "about" section of the profile that he was in a relationship with @Wisteria_Frost (display name Violette Wisteria). Open-source review of Gab revealed that @RealJM1993 is a private account but has some posts that are viewable publicly because they were reposted by user @Wisteria_Frost, including the following posts:

a. On May 14, 2023, user @RealJM1993 (James Morgan) posted: "@Wisteria_Frost Put that nigger on a tree." That post also indicated that it was associated with a "home" for "Proud racists."



b. On May 21, 2023, user @RealJM1993 (James Morgan) posted: "I think it's about time we Americans had a heart to heart talk about our jewish problem."

c. On May 29, 2023, user @RealJM1993 posted: "I think US law should only protect US citizens. If you kill an illegal, I think literally nothing should happen to you."

39. Records provided from Meta for Facebook UIDs 100001379619317 and 103661114323862 and Instagram UID 41124491714, prior to the time those accounts were closed, associated Karactus Blome with Internet Protocol (IP) address logs resolving to Charter Communications and verified phone number 608-322-5087 resolving to US Cellular.

40. On August 18, 2022, US Cellular provided records for subscriber Karactus Blome including the device as a Motorola Moto G Power, IMEI 356891111307451. The videos he posted all appear to be consistent with videos captured using a mobile phone. I know from my training and experience that photos and videos like those posted by Blome are often backed up to Google servers, uploaded to cloud based storage media, and synced to new devices.

41. On or about July 22, 2022, and June 23, 2023, the FBI sent preservation requests to Google under 18 U.S.C. § 2703(f).

42. On August 5, 2022, Google responded to a subpoena and identified Karactus Blome as the subscriber of YouTube channel UC62TCz6JDjwzqnY6Jq18EKg and email addresses clustergeek64@gmail.com and hounddowg1@gmail.com. Blome's email accounts hounddowg1@gmail.com and clustergeek64@gmail.com have been used, respectively, since March 18, 2012, and February 6, 2014. Google confirmed that the YouTube channel and email accounts remain active. The most recent physical address associated with Blome's Google accounts was 291 N Fraternity Lane #209, Whitewater, Wisconsin.

43. Records provided by multiple firearms retailers in response to subpoenas showed that clustergeek64@gmail.com was the email address associated with firearms purchases made by Blome from April 15, 2020, to June 10, 2022.

44. Records provided by Charter Communications on September 16, 2022, listed Blome's billing address as 291 N Fraternity Lane, Apt. #209, Whitewater, WI for posts made on July 2, 2022. Additionally, posts made on July 27, 2022, and August 3, 2022, return to the service address of 291 N Fraternity Lane, Suite B, Whitewater, WI, consistent with community internet service provided by the Fox Meadows apartment complex.

45. Records provided on October 5, 2022, from UW-Whitewater listed Blome's current address as 291 N Fraternity Lane, Apt. #209, Whitewater, WI.

46. As of June 12, 2023, FBI physical surveillance observed a white Honda Accord bearing Wisconsin license plate AJN9507 (registered to James Morgan) and black Ford Ranger bearing Wisconsin license plate TF4493 (registered to James Morgan) located in the parking lot of the Fox Meadow Apartments, 291 N Fraternity Lane, Whitewater, Wisconsin.

47. Based on my training and experience, there is reason to believe that the Google accounts likely contain emails and other information related to the offenses described above that cannot be obtained through means other than a search of those Google accounts.

BACKGROUND CONCERNING GOOGLE

48. Google is a United States Company that offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser called Google Chrome and a free search engine called Google Search.

49. In addition, Google offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Google also sells devices, including laptops, mobile phones, tablets, smart speakers, security cameras, and wireless routers. Users of Android and Google devices are prompted to connect their device to a Google Account when they first turn on the device.

50. Signing up for a Google Account automatically generates an email address at the domain gmail.com. That email address will be the log-in username for access to the Google Account.

51. Google advertises its services as "One Account. All of Google working for you." Once logged into a Google Account, a user can connect to Google's full suite of services offered to the

public, some of which are described in further detail below. In addition, Google keeps certain records indicating ownership and usage of the Google Account across services, described further after the description of services below.

52. **GMAIL**: Google provides email services (called Gmail) to Google Accounts through email addresses at gmail.com. Gmail can be accessed through a web browser or a mobile application. Additional email addresses ("recovery," "secondary," "forwarding," or "alternate" email addresses) can be associated with the Google Account by the user. Google preserves emails associated with a Google Account indefinitely, unless the user deletes them.

53. **CONTACTS**: Google provides an address book for Google Accounts through Google Contacts. Google Contacts stores contacts the user affirmatively adds to the address book, as well as contacts the user has interacted with in Google products. Users can send messages to more than one contact at a time by manually creating a group within Google Contacts or communicate with an email distribution list called a Google Group. Users have the option to sync their mobile phone or device address book so it is stored in Google Contacts. Google preserves contacts indefinitely, unless the user deletes them.

54. **CALENDAR**: Google provides an appointment book for Google Accounts through Google Calendar. Users can create events or RSVP to events created by others in Google Calendar. Google Calendar can be set to generate reminder emails or alarms about events or tasks, repeat events at specified intervals, track RSVPs, and auto-schedule appointments to complete periodic goals (like running three times a week). A single Google Account can set up multiple calendars. An entire calendar can be shared with other Google Accounts by the user or made public so anyone can access it. Users have the option to sync their mobile phone or device address book so it is stored in Google Calendar. Google preserves appointments indefinitely, unless the user deletes them.

55. **GOOGLE KEEP**: Google also provides online to-do lists and notepads for Google Accounts. Google Keep allows users to create notes or lists. These notes can be shared with other users to edit. Users can set notifications at particular dates and times for both tasks and notes. Google preserves tasks and notes indefinitely, unless the user deletes them.

56. **WEB-BASED CHATS and MOBILE MESSAGING**: Google provides a number of direct messaging services accessible through a browser or mobile application, including Duo, Messages, Hangouts (Chat and Meet), and the now-retired Allo and Chat. These services enable real-time communications. Users can send and receive text messages, videos, photos, locations, links, and contacts from their Google Account using these services. Chat and Hangouts require or required the other user to also have a Google Account. Duo, Messages, and Allo do or did not. Google preserves messages sent through these services indefinitely, unless the user turns off the setting to save conversation history or deletes the message.

57. **GOOGLE DRIVE**: Google Drive is a cloud storage service automatically created for each Google Account. Users can store an unlimited number of documents created by Google productivity applications like Google Docs (Google's word processor), Google Sheets (Google's spreadsheet program), Google Forms (Google's web form service), and Google Slides (Google's presentation program). Users can also upload files to Google Drive, including photos, videos, PDFs, and text documents, until they hit the storage limit. Users can also set up their personal computer or mobile phone to automatically back up files to their Google Drive Account. Each user gets 15 gigabytes of space for free on servers controlled by Google and may purchase more through a subscription plan called Google One. In addition, Google Drive allows users to share their stored files and documents with up to 100 people and grant those with access the ability to edit or comment. Google maintains a record of who made changes when to documents edited in Google productivity

applications. Documents shared with a user are saved in their Google Drive in a folder called "Shared with me." Google preserves files stored in Google Drive indefinitely, unless the user deletes them.

58. **GOOGLE DRIVE FOR ANDROID USERS**: Android device users can also use Google Drive to backup certain data from their device. Android backups on Google Drive may include mobile application data, device settings, and file downloads. If a user subscribes to Google's cloud storage service, Google One, they can opt to back up all the data from their device to Google Drive.

59. **GOOGLE PHOTOS**: Google offers a cloud-based photo and video storage service called Google Photos. Users can share or receive photos and videos with others. Google Photos can be trained to recognize individuals, places, and objects in photos and videos and automatically tag them for easy retrieval via a search bar. Users have the option to sync their mobile phone or device photos to Google Photos. Google preserves files stored in Google Photos indefinitely, unless the user deletes them.

60. **GOOGLE MAPS and GOOGLE TRIPS**: Google offers a map service called Google Maps that can be searched for addresses or points of interest. Google Maps can provide users with turn-by-turn directions from one location to another using a range of transportation options (driving, biking, walking, etc.) and real-time traffic updates. Users can share their real-time location with others through Google Maps by using the Location Sharing feature. And users can find and plan an itinerary using Google Trips. A Google Account is not required to use Google Maps, but if users log into their Google Account while using Google Maps, they can save locations to their account, keep a history of their Google Maps searches, and create personalized maps using Google My Maps. Google stores Maps data indefinitely, unless the user deletes it.

61. **GOOGLE PLAY**: Google Accounts can buy electronic media, like books, movies, music, and mobile applications from the Google Play Store. Google Play records can include records of

whether a particular application has been or is currently installed on a device. Users cannot delete records of Google Play transactions without deleting their entire Google Account.

62. **GOOGLE VOICE**: Google offers a service called Google Voice through which a Google Account can be assigned a telephone number that can be used to make, record, and forward phone calls and send, receive, store, and forward SMS and MMS messages from a web browser, mobile phone, or landline. Google Voice also includes a voicemail service. Records are stored indefinitely, unless the user deletes them.

63. **GOOGLE CHROME**: Google offers a free web browser service called Google Chrome that facilitates access to the Internet. Chrome retains a record of a user's browsing history and allows users to save favorite sites as bookmarks for easy access. If a user is logged into their Google Account on Chrome and has the appropriate settings enabled, their browsing history, bookmarks, and other browser settings may be saved to their Google Account.

64. **YOUTUBE**: Google also offers a video platform called YouTube that offers Google Accounts the ability to upload videos and share them with others. Users can create a YouTube channel where they can upload videos, leave comments, and create playlists available to the public. Users can subscribe to the YouTube channels of others, search for videos, save favorite videos, like videos, share videos with others, and save videos to watch later. More than one user can share control of a YouTube channel. YouTube may keep track of a user's searches, watch history, likes, comments, and change history to posted videos.

65. **INTEGRATION OF GOOGLE SERVICES**: Google integrates these various services to make it easier for Google Accounts to access the full Google suite of services. Users accessing their Google Account through their browser can toggle between Google Services via a toolbar displayed on the top of most Google service pages, including Gmail and Drive. Google Hangout and Chat

conversations pop up within the same browser window as Gmail. Attachments in Gmail are displayed with a button that allows the user to save the attachment directly to Google Drive. If someone shares a document with a Google Account user in Google Docs, the contact information for that individual will be saved in the user's Google Contacts. Google Voice voicemail transcripts and missed call notifications can be sent to a user's Gmail account. And if a user logs into their Google Account on the Chrome browser, their subsequent Chrome browser and Google Search activity is associated with that Google Account, depending on user settings.

Google Account Records:

66. **SUBSCRIBER RECORDS**: When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information, including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

67. **ACCESS RECORDS**: Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website or using a mobile application), and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's terms of service, as well as the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the Google Account.

68. Google maintains the communications, files, and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a communication or file from their Google Account, it may continue to be available on Google's servers for a certain period of time.

69. **BROWSING, SEARCH, and APPLICATION USE HISTORY**: Google collects and retains data about searches that users conduct within their own Google Account or using the Google Search service, including voice queries made to Google Assistant. Google also has the capacity to track the websites visited using its Google Chrome web browser service, applications used by Android users, and the use of Google applications by iPhone users. According to Google, this search, browsing, and application use history may be associated with a Google Account when the user is logged into their Google Account on the browser or device and certain global settings are enabled, such as Web & App Activity. Google also collects and retains data about the voice queries made to its artificial intelligence-powered virtual assistant, Google Assistant, on Android devices and associated it with the registered Google Account if certain global settings are enabled, such as Voice & Audio Activity tracking. Google usually maintains these records indefinitely, unless the user deletes them.

70. **LOCATION HISTORY**: Google collects and retains data about the location at which Google Account services are accessed from any mobile device, as well as the periodic location of Android devices, regardless of service usage. This location data can derive from a range of sources, including GPS data, Wi-Fi access points, cell-site locations, geolocation of IP addresses, sensor data, user searches, and Bluetooth beacons within range of the device. According to Google, this location data may be associated with the Google Account signed-in or registered to the device when Location Services are activated on the device and the user has enabled certain global settings for their Google Account, such as Location History or Web & App Activity tracking. The data retained may be both

precision location data, like latitude and longitude coordinates derived from GPS, and inferential location data, such as the inference that a Google Account is in New York because it conducts a series of searches about places to eat in New York and directions from one New York location to another. Google maintains these records indefinitely, unless the user deletes it or [not yet implemented: opts into automatic deletion of their location history every three or eighteen months.]

71. **ANDROID DEVICE DATA**: When an individual uses an Android device for the first time, they are prompted to register the device to a new or existing Google Account. Data about the use of the Android device is saved to the registered Google Account, including device characteristics such as the device serial number, model type/number, and international mobile equipment identity (IMEI). In addition, users may opt-in to Android device backups to Google cloud servers. Android device backups are only saved as a unique backup file if the user subscribes to Google's cloud storage service, Google One. If they do not, data from the device is associated with the registered Google Account and stored with similar data in the Google Account. For example, photos and videos on the device are backed up to Google Photos; contacts are backed up to Google Contacts; events and appointments are backed up to Google Calendar; and files and certain application data are backed up to Google Drive. Google maintains these records indefinitely, though users may delete Android back-up files in the same manner as any other file associated with the relevant Google service.

72. Google also maintains records of the device characteristics of iPhones used to access Google services, including the make and model of the device. Depending on user settings, those records may be associated with the Google Account logged into the service in use on the device. Google maintains these records indefinitely, unless the user deletes them.

73. In my training and experience, evidence of who was using a Google Account, and from where, and evidence related to criminal activity of the kind described above, may be found in the files

and records described above. This evidence may establish the "who, what, where, when, why, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. This can be true even if subscribers insert false information to conceal their identity; this information often nevertheless provides clues to their identity, location or illicit activities.

74. For example, the stored communications and files connected to a Google account may provide direct evidence of the offenses under investigation. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

75. In addition, the user's account activity, logs, stored electronic communications, location history, and other data retained by Google can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

76. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may

indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

77. Other information connected to a Google Account may lead to the discovery of additional evidence. For example, the identification of apps downloaded from the Google Play Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, location information, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

CONCLUSION

78. Based on the forgoing, I request that the Court issue the proposed search warrant.

79. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with YouTube channel UC62TCz6JDjwzqnY6Jq18EKg and email accounts clustergeek64@gmail.com and hounddowg1@gmail.com (the "accounts"), as well as all Google, LLC accounts linked to these accounts by cookie values, creation IP addresses, recovery email, SMS recovery, device, telephone numbers, and other similar identifiers, that is stored at premises owned, maintained, controlled, or operated by Google, LLC, a company headquartered at 1600 Amphitheater Parkway, Mountain View, CA 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google LLC (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to requests made under 18 U.S.C. § 2703(f) on or about July 22, 2022, and June 23, 2023, the Provider is required to disclose to the government the following information from August 1, 2019, to the present for each account or identifier listed in Attachment A:

Google Account

- **SUBSCRIBER AND ACCESS RECORDS:** All business records and subscriber information, in any form kept, pertaining to the account, including: full name; physical address; telephone numbers, including SMS recovery and alternate sign-in numbers; alternative and recovery email addresses, including those provided during registration; usernames, screennames and other identifiers; account status; account creation date; account registration IP address; length of service; records of session times and durations, including log-in IP addresses; methods of connecting; log files; subscriber change history; means and source of payment (including any credit or bank account number); and detailed billing records;
- **DEVICES:** All device information associated with the accounts, including but not limited to, manufacture names, model numbers, serial number, media access control (MAC) addresses, international mobile equipment identifier (IMEI) numbers, FCC ID numbers, Android IDs, and telephone numbers;
- **SERVICES:** The types of services utilized, including connected applications and sites, and any dates associated with the commencement or termination of that use;
- **FORWARDING OR FETCHING ACCOUNTS:** All forwarding or fetching accounts relating to the accounts;

- **BROWSING, SEARCH, and APPLICATION USE HISTORY:** All Internet search, browsing history, and application usage history, such as Web & App Activity**,** including: search terms; browsing history, including application usage; bookmarks; passwords; autofill information; alerts, subscriptions, and other automated searches, including associated notifications and creation dates; all text typed into the Google Chrome address bar or Google search bar, including URLs and IP addresses; all URLs or IP addresses clicked on; user settings; and all associated logs and change history;

- **LOCATION HISTORY:** All records indicating the location at which the account was active, such as Location History and Web & App Activity, including: GPS data; cell site/cell tower information; IP addresses; information associated with each location record, including the source of the data, date and time, latitude and longitude, estimated accuracy, device and platform, and inferences drawn from sensor data (such as whether a user was at rest, walking, biking, or in a car); and associated logs and user settings, including Timeline access logs and change history;

Gmail

- **GMAIL:** The contents of all emails associated with the account, including, but not limited to: stored or preserved copies of emails sent to and from the account, draft emails, and deleted emails; attachments; the source and destination addresses associated with each email; the date and time at which each email was sent; the size and length of each email; and true and accurate header information including the actual IP addresses of the sender and recipients of the emails;

- **CONTACTS:** Any records pertaining to the user's contacts, including: address books; contact lists, including autocomplete suggestions; social network links; groups, including Google Groups to which the user belongs or communicates with; user settings; and all associated logs and change history;

- **CALENDAR:** Any records pertaining to the user's calendar, including: Google Calendar entries; Google Tasks; reminders; appointments; invites; and goals; the sender and recipients of any event invitation, reminder, appointment, or task; user settings; and all associated logs and change history;

- **WEB-BASED CHATS:** The contents of all chats associated with the account, including Google Hangouts, Meet, and Chat, in any format (text, audio, or video) including, but not limited to: stored, deleted, and draft chat communications, including attachments and links; the source and destination addresses associated with each communication, including IP addresses; the size and length of each communication; user settings; and all associated logs, including access logs and change history;

Google Drive

- The contents of all records associated with the account in Google Drive (including Docs, Sheets, Forms, and Slides) and Google Keep, including: files, folders, media, notes, lists, applications, and other data uploaded, created, stored, or shared with the account including drafts and deleted records; third-party application data and backups; SMS data

and device backups; the creation and change history of each record; accounts with access to or which previously accessed each record; any location, device, other Google service (such as Google Classroom or Google Group), or third-party application associated with each record; and all associated logs, including access logs and IP addresses, of each record;

Google Photos

- The contents of all media associated with the account in Google Photos or Picasa, including: photos, GIFs, videos, animations, collages, icons, or other data uploaded, created, stored, or shared with the account, including drafts and deleted records; third-party data; the creation and change history of each record; accounts with access to or which previously accessed each record; any location, device, or third-party application data associated with each record; and all associated logs, including access logs and IP addresses, of each record;

Google Maps and Trips

- All maps data associated with the account, including Google Maps and Google Trips, including: all saved, starred, and privately labeled locations; search history; routes begun; routes completed; mode of transit used for directions; information associated with locations and other data associated with My Maps and Location Sharing; accounts and identifiers receiving or sending Location Sharing information to the account; changes and edits to public places; and all associated logs, including IP addresses, location data, and timestamps, and change history;

Google Play Store

- All activity relating to Google Play, including: downloaded, installed, purchased, used, and deleted applications, movies, music, television shows, books, magazines, games, and other files; details of the associated device and Android ID for each application, medium, or file; payment transactions; user settings; and all associated logs, including IP addresses, location data, timestamps, and change history;

Messaging Services

- **MOBILE MESSAGING:** The contents of all messages associated with the account, including Google Duo, Android Messages, and Google Allo, in any format (e.g. SMS, MMS, or RCS) including, but not limited to: stored, deleted, and draft messages, including attachments and links; the source and destination addresses associated with each communication, including IP addresses and telephone numbers; the size and length of each communication; associated telephone numbers, including SMS recovery numbers; usernames and other identifiers; user settings; and all associated logs and change history;

YouTube

- **YOUTUBE CONTENTS:** The contents of all media associated with the account on YouTube, whether active, deleted, or in draft, including: copies of videos and other

media only if uploaded to, saved to, shared by or shared with the account; edits, comments, likes, chats, and other interactions, including associated URLs; search history; channels; subscriptions; subscribers, friends, and other contacts; playlists; connected applications; associated URLs for each record; creation and change history; privacy settings for each record; and all associated logs, including IP addresses, locations, timestamps, and device identifiers;

- **YOUTUBE WATCH HISTORY:** A record of the account's watch history, including: accessed URLs and their associated duration, privacy settings, upload timestamps, tags, IP addresses, change history, location information, and uploading account or identifier; the logs for each access by the account, including IP address, location, timestamp, and device identifier; and change history;

- **YOUTUBE SUBSCRIBER RECORDS:** All business and subscriber records associated with the account on YouTube, including birthday; name; username and other identifiers; linked accounts; alternate or recovery emails; telephone numbers, including SMS recovery numbers; physical addresses; account status; account creation date; account registration IP address; length of service; means and source of payment (including any credit or bank account number); associated devices; associated Android IDs; and associated logs and change history;

AdSense and AdWords

- **ADWORDS/GOOGLE ADS:** All records for advertising transactions by the account relating to Google Ads, AdWords, and DoubleClick for Advertisers, including: bid, location of advertisement (including URL), permitted advertisements, blocked advertisements, design and customization settings, and engagement records; payment transactions; user settings; and all associated logs, including IP addresses, location data, timestamps, and change history;

- **ADVERTISING SUBSCRIBER RECORDS:** All business and subscriber records associated with the account on AdSense, Google Ads, Adwords, and DoubleClick by Google, including: name; user name; physical address; alternate or recovery emails; telephone numbers, including SMS recovery numbers; linked accounts; account status; account creation date; account registration IP address; length of service; associated devices; associated AndroidIDs; means and source of payment (including any credit or bank account number); and all associated logs and change history;

Connected Applications and Accounts

- **LINKED NON-GOOGLE ACCOUNTS:** All records relating to connected applications and websites not controlled by Google, including: applications and websites connected to the account at any time; associated account identifiers; privacy settings and account access permissions; and all associated logs, including access logs using Google credentials, timestamps, IP addresses, and change history;

The Provider is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and/or instrumentalities of violations of 18 U.S.C. § 842(p) (teaching or demonstrating the making or use of weapons of mass destruction) involving James Morgan (aka Karactus Blome) and occurring after August 1, 2019, including, for each account or identifier listed on Attachment A, information referring or relating to the following matters:

(a) Records of communications related to public and private comments posted to YouTube channel UC62TCz6JDjwzqnY6Jq18EKg including official copies of all videos posted and deleted;

(b) The identity of the person(s) who created or used the accounts, including records that help reveal the whereabouts of such person(s);

(c) Evidence indicating how and when the accounts were accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the account owner;

(d) Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information); and

(e) Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google, LLC and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google, LLC. The attached records consist of _____ [GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google, LLC, and they were made by Google, LLC as a regular practice; and

b. such records were generated by Google LLC's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google, LLC in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Google, LLC, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

_____ _____

Date Signature